Published and Copyright (c) 1999 - 2014
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1609 02/28/14

~ Senator: Ban Bitcoin! ~ People Are Talking! ~ RSA Conference 2014!

~ Facebook Email Is Gone! ~ Google Glass Driver Ban ~ Xbox One Twitch!

~ Titanfall Beta Launched! ~ Macs Are Hack Vulnerable ~ Win 8.1 When XP Ends!

~ Anti-Google Glass Attack ~ Google Kills Flip Switch ~ Adobe Backs ConnectED

-* Bitcoin Exchange Site Offline *-
-* Nintendo Wins 3DS Infringement Case *-
-* Snowden Update: Yahoo Webcam Images Stored *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Due to time constraints, there won't be any commentary in this week's issue - enjoy!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Xbox One Twitch Streaming!
"""""""""""""""""""""""""""""""" Titanfall Beta Aims for Smooth Launch!
Nintendo Wins 3DS Infringement Case!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Xbox One Twitch Streaming: All The Details

As you may have heard earlier, Microsoft has announced that the Xbox One will get Twitch gameplay streaming on March 11, just in time for Titanfall. We have more details on how this highly anticipated addition will work.

First, the Xbox One's Kinect will play a role in streaming on Twitch. By calling out "Xbox, Broadcast," the system will immediately begin streaming, and calling out "Stop Broadcast" will end it. Kinect will also allow picture-in-picture video feeds and audio commentary through its microphones and cameras.

Streaming works from any source, even the PS4, so you're able to enjoy content from anything that connects to Twitch. You'll also be able to archive gameplay and access any archived Twitch content from the console.

Outside of streaming, you'll be able to chat with other streamers and even join in on their games. Chat streams are fully available, a full 10 lines are displayed, and commenting even supports emotes and badges. You can even join broadcaster parties.

Finally, you'll be able to check in on friends' broadcast status in the Xbox One friends app. Notifications are available to let you know when a favorite stream starts.

Titanfall Beta Aims for Smooth Launch Avoiding EA s Previous Problems

Let s break it. These are the words said to Respawn head Vince Zampella by programmer Jon Slothy Shiring, ready to push servers to their limits. Over Valentine s Day weekend and into the following Wednesday, Titanfall launched a public beta on both the Xbox One and PC. Initially being a closed beta requiring a code, these three words inspired the team at Respawn to swing wide the doors and let all Xbox owners in to see the game. The move was nothing short of encouraging, especially coming off of the seven-and-a-half hour server issue that kept many people from playing on Valentine s Day.

Titanfall is being published by Electronic Arts, a company that has not made a good reputation for itself this past year. The problems started first with the launch of SimCity, which became a textbook example of bad PR and even worse launch preparedness. Months later, Battlefield 4 would encounter heavy server and stability issues across all platforms, leading people to accuse EA of pushing out unfinished software in an attempt to grab gamers from Call of Duty. The title is still undergoing heavy maintenance, even grinding DLC production to a screeching halt in an attempt to focus on playability issues. With such a lackluster 2013 fresh in the minds of gamers, there has been heavy skepticism about the reliability of Titanfall come launch.

And who can blame them? As an early adopter of both titles, I myself was extremely worried about the state of Titanfall on release. I experienced the silent stripping away of servers on Battlefield 3, which gutted the game and requested that players join custom matches. I was among those who got roped into the microtransactions that have been imposed onto a multitude of EA titles, including Mass Effect 3 and Dead Space 3. For two years in a row, they have stripped away consumer confidence and been voted Worst Company in America. How can we trust them, and how can we come to expect something better this spring?

Leave that to Respawn Entertainment. It s the Let s break it attitude that should give gamers the most confidence come March 11th.

Nintendo Wins 3DS Infringement Case

After a year-and-a-half in the court system, Nintendo announced today that

it won a patent infringement case at the International Trade Commission brought forth by Technology Properties Limited LLC, Phoenix Digital Solutions LLC and Patriot Scientific Corp.

In July 2012, the three patent-licensing companies filed a complaint against Nintendo for infringing upon their high-performance, low-cost microprocessor patents allegedy used in the company’s handheld systems. But the trade commission found that Nintendo didn’t infringe on any of the patents with its 3DS and DSi systems.

"We are very pleased with the commission s determination, which confirmed the judge s finding that Nintendo s products do not infringe the asserted patent, said Richard Medway, vice president and deputy general counsel at Nintendo of America. Nintendo s track record demonstrates that we vigorously defend patent lawsuits, including cases in the ITC, when we believe we have not infringed another party s patent."

Last month, IGN reported on how Nintendo must forfeit a percentage of 3DS sales to Tomita Technologies due to a lawsuit regarding the 3D stereoscopic display technology. Nintendo pays 1.82 percent of the handheld system’s wholesale price to Tomita.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

RSA Conference 2014: A Call To Arms, After A Dismal Year for Cyber Security

While thousands of tech companies and organizations, big and small, and many more concerned citizens got out and protested mass internet surveillance earlier this month, one senior VP at a security firm told attendees at this week’s RSA Conference on cyber security that they aren’t mad enough.

In what could be seen as a "call to arms" address to the cyber security community, VP and general manager of Juniper Systems business security division Nawaf Bitar told the cyber security community assembled at the annual RSA Conference on Tuesday that they weren’t doing enough.

"Our privacy is being invaded, our IP is being stolen, the public trust is at an all-time low, and the attack on our information is outrageous," said Bitar during his keynote address at the RSA Conference 2014 in San Francisco, CA, according to Information Week. "But you know what? I don’t think we give a damn. I’m fed up with talking about outrage."

Bitar pointed out that much of the "outrage" being expressed by the cyber security community (and modern society in general) over recent revelations of mass surveillance and other growing threats to everyday cyber security is rather feeble, especially compared to historical acts of protest like the Tiananmen Square protests and Tibetan monks protesting war with suicide by fire. Instead, he called the current

engagement against surveillance and privacy threats "first world outrage."

"'Liking' a cause on Facebook is not outrage. Retweeting a link is not outrage. Posting a bad review is not outrage," intoned Bitar, according to IW's report, before taking aim at cyber security officials who boycotted the RSA Conference 2014 after revelations broke that the major security company accepted money from the National Security Agency to deliberately weaken encryption standards: "Not showing up at a conference is not outrage."

Last year was probably the worst on record for cyber security and the community of experts charged with maintaining it. Starting in the summer of 2013, revelations leaked by ex-NSA contractor Edward Snowden led to a veritable avalanche of revelations about the U.S. government's deep and wide compromising of cyber security, nationwide and around the world.

Add to that the numerous high-profile hacking and data theft cases that cropped up in 2013, continuing cyber threats from foreign nations like Iran and China, topped by the end-of-year credit card breach at Target stores - which left over 100 million customers vulnerable to theft and fraud - and you end up with something of a moral crisis for the cyber security community.

"You in this room have to do better," said Bitar on Tuesday. "We're complicit -standing by and watching a crime."

Bitar continued, "We should be truly outraged, not first-world outraged. The time for apathy is over. We cannot go on the offensive and hack back, but we can no longer remain passive. It's time for a new type of offense - a type of active defense that disrupts the economics of hacking and challenges convention. It's time for all of us to turn the tables on the attackers."

In his speech, Bitar didn't provide many details on how the cyber security community could approach an "active defense," other than pointing out that many ideas in cyber security are now outdated and urging radical innovation in the industry, which drew some skepticism from the crowd.

But he did make an emphatic point about what's at stake, displaying an image of a mushroom cloud in his presentation, according to PC Mag, and saying, "It's time for all of us to turn the tables on the attackers... Or we can wait for the next world war to begin in Silicon Valley."

Website of Bitcoin Exchange Mt. Gox Offline

The website of major bitcoin exchange Mt. Gox is offline Tuesday amid reports it suffered a debilitating theft, a new setback for efforts to gain legitimacy for the virtual currency.

The URL of Tokyo-based Mt. Gox was returning a blank page. The disappearance of the site follows the resignation Sunday of Mt. Gox CEO Mark Karpeles from the board of the Bitcoin Foundation, a group seeking legitimacy for the currency.

At the Tokyo office tower housing Mt. Gox, bitcoin trader Kolin Burgess

said he had picketed the building since Feb. 14 after flying in from London, hoping to get back $320,000 he has tied up in bitcoins with Mt Gox.

"I may have lost all of my money," said Burgess, next to placards asking if Mt. Gox is bankrupt. "It hasn't shaken my trust in Bitcoin, but it has shaken my trust in bitcoin exchanges."

A "crisis strategy" report shared widely online that purports to be an internal Mt. Gox document says more than 740,000 bitcoins are missing from the exchange, which froze withdrawals earlier this month. It says the theft went unnoticed for several years and turned on disguised withdrawals.

A theft of that magnitude would equate to losses of $350 million at current bitcoin prices, but in practice such a figure is highly uncertain because of Bitcoin's extreme fluctuations in value and its lack of broad acceptance as an alternative to money.

The cloud hanging over Mt. Gox is a possibly fatal blow to Bitcoin, which was started in 2009 as a currency free from government controls. Supporters have said Bitcoin's cryptography makes it immune to theft or counterfeiting.

On bitcoin exchanges, the currency's value has fallen to about $470 from $550 in the past few hours.

Several bitcoin exchanges and related organizations released a joint statement that said they are working to "re-establish the trust squandered" by the failings of Mt. Gox.

The bitcoin operators said funds under their control are held securely. Mt. Gox should not be considered a reflection of the value of Bitcoin or the digital currency industry, they said.

A second man protesting outside Mt. Gox's office in Tokyo said he was in arbitrage, which is a type of trading, but would only gave his first name, Aaron.

A security officer said no one from Mt. Gox was in the building. Tibbane, an Internet company that Karpeles is CEO of, still has its named listed on the building's directory.

"I have no idea" where they are, said Burgess. "I'm both annoyed and worried"

Bitcoin had been inching toward broader acceptance despite wild swings in value in the past year. For most of the currency's history, each digital coin had been worth less than $10.

New bitcoins are "mined" or generated by computers. They get harder to generate all the time, which means the inflow of fresh bitcoins keeps falling.

There are about 12.4 million bitcoins in circulation today, according to Blockchain, a public registry of bitcoin transactions. The maximum number of bitcoins that can be generated is 21 million and by 2032, 99 percent of those will have been created.

Senator Calls For Total Ban of ’Dangerous’ Bitcoin

Sen. Joe Manchin, D-W.Va, has written to federal regulators urging them to totally ban Bitcoin, the "cryptocurrency" that has so excited the financial and tech world over the last year. Manchin calls Bitcoin "dangerous," "disruptive" and "highly unstable."

Addressed to Treasury Secretary Jack Lew and several other regulators, the letter paints Bitcoin as volatile and unregulated, a criminal currency already denounced by other major governments.

"The clear ends of Bitcoin for either transacting in illegal goods and services or speculative gambling make me weary of its use," Manchin, who sits on the Senate Banking Committee, concludes. "I urge the regulators to work together, act quickly, and prohibit this dangerous currency from harming hard-working Americans."

Sen. Manchin’s objection certainly comes at a time of major turmoil in the virtual currency’s history: The largest Bitcoin exchange (at which coins can be bought, sold, and traded), Mt. Gox, collapsed earlier this week after months of problems. Federal prosecutors are already looking into it and have reportedly issued subpoenas to Mt. Gox and others.

And the volatility of the currency is indisputable: Bitcoins went from being worth $20 each to over $1200 over the course of a year, before settling on their present value at around $500.

Silk Road, the most commonly cited marketplace for buying illegal goods with Bitcoins, also recently went under while at the same time, major e-commerce sites like Tiger Direct and Overstock.com have begun accepting Bitcoin and are doing quite a bit of business with it.

Snowden Update: British, American Spies ’Stored Millions of Yahoo Webcam Images’

Britain s communications spy agency GCHQ and the US National Security Agency (NSA) intercepted and stored images from webcams used by millions of Yahoo users, the Guardian newspaper reported on Thursday.

GCHQ files leaked by former NSA contractor Edward Snowden reportedly revealed how the Optic Nerve program collected still images of webcam chats regardless of whether individual users were suspects or not.

In one six-month period in 2008, the British spy agency collected webcam imagery from more than 1.8 million Yahoo user accounts around the world, the Guardian said.

Yahoo, which was apparently chosen because its webcam system was known to be used by GCHQ targets, expressed outrage at the reported surveillance.

"We were not aware of nor would we condone this reported activity," a spokeswoman for the US technology firm told AFP in an email statement.

"This report, if true, represents a whole new level of violation of our users privacy that is completely unacceptable. We are committed to

preserving our users trust and security and continue our efforts to expand encryption across all of our services."

Leaked GCHQ documents from 2008 to 2010 explicitly refer to the surveillance program, although the Guardian said later information suggests it was still active in 2012.

The data was used for experiments in automated facial recognition, as well as to monitor existing GCHQ targets and discover new ones, the British paper said.

The program reportedly saved one image every five minutes from a webcam user s feed, partly to comply with human rights legislation and partly to cut down the sheer amount of data being collected.

GCHQ analysts were able to search the metadata, such as location and length of webcam chat, and they could view the actual images where the username was similar to a surveillance target.

The data collected, which was available to NSA analysts through routine information sharing, contained a significant amount of sexual content, the newspaper added.

It cited one document as saying: It would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person.

In a statement to the Guardian, GCHQ said all of its work was carried out in accordance with a strict legal and policy framework which ensures that our activities are authorized, necessary and proportionate .

Mac Computers Are Vulnerable to Hacking; Fix Will Be Released Very Soon

Apple said Monday it was developing a security fix for its OS X computer operating system after a patch released for its iPhones and iPads to thwart hacker attacks.

The California tech giant released its security update for the iOS 7 mobile operating system Friday, saying that an attacker with a privileged network position may capture or modify data in a browsing session.

Security experts pointed out over the weekend that the same problem could affect people using Mac desktop or notebook computers.

An Apple spokesman told AFP, when asked about the Mac OS vulnerability, We are aware of this issue and already have a software fix that will be released very soon.

Security researcher Graham Cluley said it was really important that you update your iPhones and iPads as quickly as possible.

Cluley said Apple s iOS update fixed a critical vulnerability that could allow hackers to intercept what should have been secure communications between your iPhone and SSL-protected websites. That means, potentially, online attackers could grab your user ID or passwords as you attempted to log into popular websites.

The first news of the flaw came from the security firm CrowdStrike in a blog post Friday.

While Apple is working on a fix for the Mac OS, some experts say users of the computers should exercise caution.

In the meantime, be careful where you browse with your OS X based machines, said Rick Wanner at the SANS Internet Storm Center.

Paul Ducklin at the British security firm Sophos said Apple is being more open than in the past on security.

The good news is that Apple has broken its usual code of silence, he said in a blog post Monday.

Sadly, (Apple) didn t define very soon, but you should watch for this patch and apply it as soon as you can.

At Apple, A Flaw, A Fix and Fears of A Damaged Brand Add to ...

For 18 months, some of Apple Inc. s most popular products contained a glaring security flaw one that had the potential to make its users vulnerable to hackers and scam artists.

The flaw has led to an outcry from numerous security experts, forced developers to rush out a software fix for iPhones, iPads and Mac personal computers, and caused the world s largest technology company much embarrassment. But will it cause a noticeable hit to the bottom line? Not likely.

Samsung didn’t deliver on the rumored 2K screen or a high-end metal body. But given the firm’s market position and financials, the incremental improvements of the Galaxy S5 make a lot of sense. Jon Gordon reports.

Late last week, amid an outcry from several security experts, Apple issued a security patch for its mobile devices, designed to fix an error that has come to be known as the Goto fail bug. This week, it released a similar patch for its Mac computers.

The glaring error can be traced back to a single line of faulty computer code. The code has to do with two network protocols: the Secure Sockets Layer (SSL) and the Transport Layer Security (TLS).

In simple terms, the protocols dictate the process by which the user s computer checks to see whether the websites the user is visiting really are what they claim to be.

For example, a high-security website, such as that of a bank, may use a secure certificate to establish that it really is the bank s site and not, say, a fake site created by an opportunistic hacker.

Because of the error in the code, certain Apple hardware and software essentially failed to perform that check properly meaning that, in certain cases, a third party could access the supposedly secure information flowing from the user to that site.

In reality, the likelihood of that happening, even with Apple s security flaw, is exceedingly low. The malicious user exploiting the vulnerability would need to have access to the wireless network that the victim uses to get online. (As such, the flaw is perhaps most dangerous for users who spend a lot of time on easily accessible networks, such as the free WiFi offered by some coffee shops, for example.)

But what alarmed many security analysts and Apple customers are the circumstances surrounding the security lapse. For one thing, the error has the potential to affect virtually any software that uses the SSL and TLS protocols to connect to the Internet. The problem also affects a range of Apple devices, from iPhones to iPads to Mac computers. Most concerning, the vulnerability has existed, unfixed, for a year and a half.

It s difficult to overstate the seriousness of this issue, wrote security expert Aldo Cortesi, who reconfigured a popular network tool to exploit the Apple error, as a means of showing how relatively easy it would be for a malicious actor to do the same.

For years, Apple computers were seen as a safe haven from the myriad viruses that plagued Windows-based machines. Indeed, many Mac computer owners bragged about the technology s relative lack of malware, bug-filled code and the so-called blue screen of death that all too often struck Windows machines.

But Apple s new security lapse about which the company has said very little, beyond issuing the software fixes comes at a time when companies such as Target and information security firm RSA have had to deal with the fallout from massive security and privacy breaches.

And yet, perhaps because of the highly technical nature of such breaches, or perhaps because many users simply don t care enough about them, Apple s error shows little sign of affecting the company s business in any significant long-term way.

Apple shares are down slightly since news of the security flaw exploded dropping about 5 per cent over five days. But the only way that Apple will suffer lasting damage is if this security flaw shows real evidence of user harm, or if it proves to be the first of many such problems, said Neil Bearse of the Queen s University School of Business.

How much do ordinary people like you and I understand the ins and outs of SSL? Not very much, Mr. Bearse said. Without any knowledge of people getting hacked, there s little damage for Apple long term.

Mark Zuckerberg Says WhatsApp Worth More Than $19 Billion

Facebook Inc. Chief Executive Officer Mark Zuckerberg said WhatsApp Inc., which his social-media company agreed to buy last week, was worth more than $19 billion.

The mobile-messaging startup was a great fit for us, Zuckerberg said at the Mobile World Congress in Barcelona yesterday. Already almost half-a-billion people love using WhatsApp for messaging and it s the most engaging app we ve ever seen exist on mobile by far.

The cash-and-stock acquisition would be the biggest by Facebook, the

world s largest social network, and the most expensive for an Internet company in more than a decade. The deal gives WhatsApp roughly the same valuation as Gap Inc. and more than half the market value of microblogging service Twitter Inc.

Zuckerberg, who also bought photo-sharing service Instagram for about $700 million in 2012, has been adding applications such as messaging and news to court smartphone and tablet users.

The WhatsApp deal will help Facebook play a more important role in getting more people connected, Zuckerberg said.

Mountain View, California-based WhatsApp, which is popular in Europe, lets users send messages through its service on mobile devices based on different operating systems including Apple Inc. s iOS, Google Inc. s Android, Microsoft Corp. s Windows Phone and BlackBerry Ltd. s software.

Unlike traditional text messages, which consumers pay for through their mobile-phone plans, WhatsApp is free for the first year, and costs 99 cents a year after that. It also competes with Tencent Holdings Ltd. s WeChat in China, KakaoTalk in Korea and Line in Japan, as well as Facebook s own application, Facebook Messenger.

While Zuckerberg declined to comment when asked whether he would make a bid for Snapchat, he said that after a large deal such as WhatsApp, you re probably done for a while.

While WhatsApp had low revenues, it would be worth more because of its strategic value, huge business potential to double its users and its fit with Facebook.

Zuckerberg also said he s seeking three to five phone companies as partners in an effort to connect billions of people to the Internet that don t yet have access.

Carriers joining the initiative would roll out networks and provide data service for free to people who can t afford it, he said. That would provide services including social networks, messaging, food and weather information that could eventually bring in revenue for carriers and Internet companies.

 I want to show that this model works, that s why we re looking for partners who are serious about this, he said. The undertaking will probably be loss-making for years. If we do something that s good for the world, we ll eventually come up with a way to make money from it.

Last August, Facebook said it s forming Internet.org, a group with other technology companies to expand access to the Internet for the 5 billion people who have yet to get online. The group includes partnerships with mobile-device makers Samsung Electronics Co. and Nokia Oyj (NOK1V), and chipmaker Qualcomm Inc. (QCOM) The group, which follows Facebook s own efforts to expand Internet access in emerging markets, intends to develop projects and mobilize industry and governments to enable more people to move online.

Zuckerberg said concerns about data security and government intervention should not affect growth of the Internet.org initiative.

 The governments have a responsibility to protect folks and also to be transparent about what they are doing, he said. I think they were way

over the line in not being transparent enough.

Anti-Google Glass Attack in San Francisco Highlights Tension Over Wearables

San Francisco social media consultant Sarah Slocum says she was attacked this weekend for using Google Glass in a local bar. On her Facebook profile, Slocum said she was verbally and physically assaulted by bar patrons who jeered at her for using Glass and, she alleges, snatched the device off of her face. Slocum also said that she was robbed after leaving her purse in the bar as she pursued her alleged attackers.

She has posted a video of part of the incident to YouTube, though it doesn t show the all the details of the alleged attack.

Another video, shared with San Francisco television station KRON4, shows one of the alleged attackers telling Slocum that people like her are destroying the city of San Francisco a comment that ties this incident into a growing backlash against tech companies such as Google, Twitter and others in the city.

San Francisco Police Department Officer Albie Esparza confirmed that a woman reported being involved in an altercation over Google Glass after they believed she was recording them without their consent in a bar Saturday at 1:45 a.m. He said that no suspects are in custody.

Wearable technology is moving people into a brave new world with new rules about how to use evermore ubiquitous gadgets. The path to acceptance, however, is not a smooth one. Google s head-mounted Glass computer, for example, faces a long road ahead to convince the general public that smart glasses will eventually be as accepted as camera-phones and earbuds. The device has many of the same functions as a smartphone, but lets users read e-mail, see notifications, get directions and take calls via a screen on their faces rather than on their smartphones.

The San Francisco incident follows a handful high-profile reports of negative, sometimes violent reactions that Google Glass users have reported as the new technology causes rifts with restaurant owners, law enforcement officials and movie theater owners.

From a legal standpoint, those fights have largely come out in Google s favor. A San Diego court dismissed a case against a woman pulled over for using Glass last month. But more cases could be on their way, as a handful of states have also discussed legislation to ban Glass behind the wheel amid worries that having a small screen hovering in users peripheral vision will pose a danger on the roads.

Education has been the main tool in Google s arsenal as it faces questions about the implications Glass has for privacy, distracted driving, piracy and a general unease among some folks who see a person walking around with a head-mounted computer.

The firm, which has already taken the tech for demonstrations on Capitol Hill, has also been touring the country and showing Glass to mayors, state legislators and the general public in order to let people know more about the benefits it sees in the technology.

Google has also placed considerable weight on its beta testers which it

calls Explorers to act as ambassadors for the technology. Last week, Google released a list of dos and don ts for Explorers to give them basic etiquette and safety tips on using the device and to remind them to be respectful when facing Glass doubters.

New technology raises new concerns which is why educating Explorers and those around them is a top priority for the Glass team, Google said in a statement. The point of the Explorer program is to get Glass in the hands of people from all walks of life and see how they use it out in the world. Our Explorers provide us with continuous feedback and on the whole, they act as positive ambassadors for Glass on a daily basis. While Glass is currently in the hands of this small group, we find that when people try it for themselves they realize Glass connects people more with the world around them than distracts them from it.

Joseph White, a Rockville-based consultant and Explorer, said that he s only faced one negative reaction to his use of Glass since he started using it in December and it was not nearly as confrontational as Slocum s alleged encounter.

The closest experience that I have had to [Slocum s] is someone coming up to me at an Organizing for America event .?.?. and asking me What are you recording right now? ? he said. White, who is in his 60s, said that while he s had some conversations with people about the privacy implications of Glass, those same people have also asked to try on the device and have their picture taken with him.

I have never been asked to take them off, he said. And I have been in restaurants, some bars just out in public at different functions.

Google Glass Ban for Drivers Wise Approach

Drivers should drive.

Yet, given all the distractions of life including constant access to information, entertainment and more on high-tech devices driving a vehicle has become, well, a secondary thought to some. Driving is a bother.

It limits the time people can email, text and talk to each other.

State legislatures, including Washington s, have made it illegal to drive while texting or talking with a cellphone held to the ear. Nevertheless, distracted driving continues to be a serious and deadly problem.

And it could get a lot worse.

Google has come out with glasses that allow wearers to access and view the Internet and take photos with literally a blink of an eye. Google Glass has the potential to garner billions in profit.

Google is pitching its eyewear device hard, hoping to market the glasses specifically for driving. It is working with carmakers to integrate the technology with their vehicles.

Google, of course, argues that Google Glass will help drivers avoid road hazards and would be less distracting than smartphones when used

properly.

That s difficult to believe. Smartphones aren t always used properly, so why would anyone believe glasses that project email in front of your eyes would be used properly? Do we really want people watching movies or cat videos in control of a 4,000-pound car going 70 mph?

Given death or permanent injury are likely outcomes for misusing high-tech devices while driving, it is essential steps are taken to limit the use of Google Glass for now.

Wisely, six state have banned or are considering banning Google Glass for drivers. Washington and Oregon should jump on board.

These ban bills could limit the marketability of Google Glass, said Richard Bennett, a visiting scholar at the Washington-based American Enterprise Institute who coinvented Wi-Fi. Driving is certainly one of the premier applications for Glass.

And these ban bills could, more importantly, also limit disaster.

Advances in technology move faster far faster than laws. Cellphones and smartphones were already in use when it became obvious that multi-tasking while driving was dangerous. Laws were put in place to limit the behavior, but many foolishly cling to the practice (convincing themselves that their texting while driving skills are better than others.

Getting ahead of Google Glass (and the similar products that are sure to follow) is a sign society is starting to accept the need to put human safety ahead of advances in technology.

Netflix May Need To Pay AT&T, Verizon for Faster Speeds

Netflix Inc, which agreed to pay Comcast Corp for faster video delivery, may have to make similar arrangements with other broadband providers to make sure its customers get trouble-free access its streaming movies and TV shows.

Verizon Communications' chief executive said on Monday he expects Netflix will pay the telecom company for faster speeds after Netflix customers complained about slow connections to stream TV shows and movies with Verizon's FiOS service.

AT&T spokesman Mark Siegel said in a statement on Monday that "we're in discussions with Netflix to establish a more direct connection between our networks, similar to agreements we have with others, so that AT&T broadband customers who use Netflix can enjoy an even better video experience."

Talks with telecom companies that provide broadband Internet access gained momentum after Sunday, when Netflix agreed to pay Comcast Corp for faster speeds.

Evercore Partners analyst Alan Gould said the agreement with Comcast removed uncertainty and likely involved small payments since Netflix agreed voluntarily to the arrangement.

"This is probably a template for the deal that will get done with other broadband providers," said Gould, who has an "overweight" rating on Netflix shares. "We are assuming the payments are not going to materially change the business model."

Verizon CEO Lowell McAdam said on CNBC, where he discussed Verizon's talks with Netflix, that the two companies have been in negotiations for a year.

These deals hinge on whether Netflix can set up direct access to Verizon, known as an "interconnect agreement," rather than go through a third party. Verizon provides millions of U.S. customers with its FiOS broadband service and Netflix speeds have slowed on that network in recent months, leading to complaints.

Many providers including Cox, Cablevision and Google Fiber directly connect to the Netflix network through a service the streaming company developed called Open Connect. Those providers have not seen their speeds deteriorate in recent months.

But others, including AT&T and Verizon, have opted not to use Open Connect.

Shares of Cogent Communications, one of the companies that took care of the Internet traffic exchange between the Comcast and Netflix networks, fell 7 percent on Monday as investors worried that these deals would take away Cogent's business.

Cogent's chief executive Dave Schaeffer played down the effect of the Comcast-Netflix agreement on its business and reaffirmed the company's annual revenue forecast.

"It doesn't mean that revenue goes away from Cogent. It just means that some of the growth in revenue may not occur through us," he said.

McAdam, the Verizon CEO, spoke out in favor of telecom companies signing deals with Netflix.

"It shows you don't necessarily need a lot of regulation in a dynamic market here. Doing these commercial deals will get good investment and good returns for both parties," McAdam said.

Asked about discussions with Verizon or other providers, Netflix spokesman Joris Evers said "we talk to all major ISPs all the time to make sure Netflix users get the best possible experience."

Google Makes Good on Threat, Flips 'Kill Switch' on Some Chrome Add-ons

Google upgraded Chrome to version 33, fulfilling its promise to block more add-ons in the Windows browser and quashing 28 bugs.

The promotion of the new tools and features to Chrome's "Stable" channel, one of three that the Mountain View, Calif. company maintains, had been trumpeted previously, and baked into rougher builds.

Top on the change list was the posting of a "No trespassing" sign: Only extensions or add-ons that originate from the Chrome Web Store, Google's

official distribution channel, can be installed. The new policy currently affects only users of the Windows version of Chrome 33.

Chrome 33 also automatically throws a "kill switch" on extensions that had been installed previously from sources other than the Chrome Web Store. Google called this a "hard-disable," or one that prevents the user from re-enabling the add-on. Some exceptions applied.

Google first promised that in November, when Erik Kay, director of Chrome engineering, cited "our continuing security efforts" for the change, and stated, "We believe this change will help those whose browser has been compromised by unwanted extensions."

Google has been tightening the screws on third-party add-ons since July 2012, when it first required that add-ons move to the Chrome Web Store. In other subsequent steps, it blocked sneaky add-on installation.

Those stricter policies had driven some purveyors of adware to try an end-around by buying the rights to established add-ons already in the Chrome Web Store, then modifying them to bombard users with advertisements.

Starting with Chrome 33 on Windows, Google is closing the remaining loopholes: Extensions that had been installed locally or by businesses internally must be published to the Chrome Web Store. Businesses can hide their extensions on the store from the public at large - or continue to use group policies to offer the add-ons to their workforce from their own servers - and developers will still be able to initiate "in-line" installs from their website, assuming the add-on is also in the Chrome Web Store.

Only add-ons that were installed via such enterprise policies or by developers from their websites or software can avoid the automatic "hard disable" that Google mandated.

By forcing add-on developers to publish their work in the Store, Google moved another step closer to a closed market, the kind popularized by Apple’s mobile app ecosystem, where it can more easily vet the extensions and then yank them if necessary.

On the Mac version of Chrome 32, add-ons that had been installed from sources other than the Chrome Web Store - such as 1Password’s extension, which was installed on one staffer’s Mac by that password management software - were not disabled but were instead marked with "Not from Chrome Web Store."

Chrome 33 also debuted notifications for Google Now, the company’s digital Siri-like assistant, within the browser on Windows and Apple’s OS X. Those notifications stem from the Android and iOS Google Now apps.

Along with the feature promotions, Google patched 28 vulnerabilities in the browser, including five rated "high," the company’s second-most-serious threat ranking. Three of the vulnerabilities were classified as "use-after-free" issues, a type of memory bug that in-house and external researchers have become adept at rooting out, largely by using Google’s own AddressSanitizer fuzzing tool.

Seven outside researchers were paid a total of $13,500 in bounties for reporting six of the 28 flaws. So far this year, Google has paid out more than $21,000 in bug bounties.

Chrome 33 also included the most-up-to-date version of Adobe’s Flash Player - Google’s browser uses an integrated edition of Flash and so updates it automatically - that was released earlier today after reports surfaced that hackers were exploiting a critical vulnerability.

People who haven’t tried Google’s desktop browser can download Chrome 33 for Windows, OS X and Linux from Google’s website. Current users can let the automatic updater download and install the new version.

Windows 8.1 Update Said To Arrive When XP Ends

Mark your calendars. Early April promises Windows updates as well as the end of support for Windows XP.

April 8 is the day support for XP ends. Though it may be cold comfort for XP users, it may also be the day that Microsoft updates Windows 8.1.

Early April is shaping up to be a watershed of sorts for Windows users. At the same time that support for Windows XP is ending, the Windows 8.1 update is arriving to the general public, according to Neowin, citing a tweet from Supersite for Windows.

That date was also suggested earlier this month.

And April 8 is also the day for Microsoft’s "Patch Tuesday," when it releases updates and fixes for a variety of Windows products.

But getting back to the Windows 8.1 update. A week before April 8, on April 2, MSDN users may be able to get the update, according to the same report.

Microsoft Vice President Joe Belfiore said at Mobile World Congress this week that the company wants to "make things better" for users without touchscreens.

Those changes may include new right-clickable context-sensitive menus, the ability to pin Metro apps to the Desktop task bar, and adding dedicated search and power buttons to the Start screen, as described earlier this month by ZDNet.

Meanwhile, the countdown for the end of support for XP continues. "There will be no more security updates or technical support for the Windows XP operating system," as Microsoft has made amply clear.

Want To Unsubscribe from A Mailing List in Gmail? Look Up, Not Down

If you interface with Gmail through a browser, Google just flipped the switch on a slick new feature so slick, in fact, that it ll make you wonder why it s not ubiquitous in email-dom.

When a promotional email graces your inbox if you have a few sitting in your Trash folder, you can follow along train your eyes on the email header, just to the right of the sender s designation. You re looking for

the word Unsubscribe. If you can find an email that looks like this, that word s just what it sounds like: an easy-peasy, one-click link that fires off an automated email to the sender requesting they remove you from further sendings. No fuss, no muss.
gmail-unsubscribe

The idea is to make it simpler to remove yourself from unwanted promotional lists, to be able to opt out without having to sort through the fine print at an email s footer or wallow through some company s proprietary (and on occasion prohibitive) removal mechanics. The feature s been around for some time in Gmail, but only for a minority of users. Google just turned it on for everyone.

Mind you, it s not a panacea. It s not clear, for instance, that an automated message from Gmail to a promotional sender is going to do the trick, since it circumvents the sender s own automated removal process. It s also not clear how Gmail differentiates between wanted and unwanted emails (or promotional versus non-promotional). The Unsubscribe option appeared in some of the promotional emails I flipped through this morning, but not others.

I wondered if it might be a simple text scrape   a process whereby Google s checking for the word unsubscribe (tied to a link) somewhere in the email   but I ve isolated several instances of promotional emails that contain the word but don t manifest Google s new Unsubscribe option that sink that theory.

It s also not designed to combat spam, say someone trying to send you your million dollar prize winnings. Those emails will continue to show up in your Spam folder; as always, your best bet s to simply zap them (never reply to spam).

In the future, wouldn t it be nice if this were intrinsic to all forms of communication? I m talking about a standard opt-out button every marketer has to comply with, that s as mandatory as the hang-up switch for a voice call, and as omnipresent as the power button on an electronic device.

Remember Your Facebook Email Address? It s Gone

Did you know you have a Facebook email address? Neither does anyone else. And that s why yesterday Facebook announced that it was retiring its public email system, which has been in existence since November 2010.

Users logging into Facebook will soon see (or have already received) the following message at the top of their screens.

Facebook offers further explanation:

What s changing with @facebook.com email addresses?

Currently, messages sent to your @facebook.com email address are delivered to your Facebook Messages.

However, we re updating the way @facebook.com email addresses work, so that soon any email messages that are sent to your @facebook.com email address will no longer go to your Facebook Messages. Instead, these emails will be forwarded to the primary email on your Facebook account. Learn how

to add or update your primary email.

As a part of this change, any current Facebook conversations that include an email address will become read-only. This means that you ll still be able to view the conversation, but you ll no longer be able to reply to it from your Facebook Messages. To continue the conversation, you can always message people through their Facebook accounts.

A Facebook spokesperson told tech news site Re/Code that the social network ditched its flagging email service because it wanted to focus on improving our mobile messaging experience. There is no mention of Facebook s recent $19 billion acquisition of uber texting service WhatsApp, but feel free to draw your own conclusions.

Any messages sent to your existing @facebook.com address will be automatically forwarded to the email address you gave Facebook when you signed up including messages from strangers that Facebook designated as other, which often include a fair amount of spam.

According to a Facebook spokesperson, Facebook will continue to run all emails through its spam filters before forwarding them. Senders will not be able to see your primary email address (unless, of course, you reply to them).

Don t like it? You will be able turn off forwarding, though instructions on how to do that have yet to be made public. According to a Facebook spokesperson, the changes should roll out in early to mid-March. At that point, you ll be able to disable forwarding.

At press time Facebook s user base had yet to throw its customary tantrum over changes to the service. Even they don t seem to care.

Adobe Backs ConnectED Initiative, Sends Free Software to Schools

Microsoft, Apple, Sprint and Verizon have already shelled out millions to help the president bring high-speed broadband to schools and amp up the role technology plays in education. Now Adobe’s on the bandwagon too, and it’s bringing along gobs of software and educational resources for kids and teachers. Students at some 15,000 US schools get access to Photoshop Elements and Premiere Elements, while the staff gets tools from Adobe’s Education Exchange, electronic signature software and presentation tech for distance learning. The company’s total commitment weighs in at over $300 million, but it’s not hard to see what it gets out of the deal. Looking past the potential for a hefty tax writeoff, the company said its plans are in line with the Common Core State Standards Initiative’s emphasis on media production and criticism. In other words, Adobe wants to help foster creative skills in youngsters. Getting a new generation of media-savvy kids interested in its production tools is just icing on the cake.

Research Shows that 87% of Americans Now Regularly Uses the Internet

You should be aware that the World Wide Web is turning 25 years old on March 12. One may wonder what have changed in a quarter of a century?

This led Pew Research Center to conduct a survey that would show how far the Web has come through the years.

It could be considered as a tribute to the World Wide Web. The release of the findings of the survey indicates how the Internet has figured in into American culture and society. It found that overwhelmingly, up to 87% of adult US citizens now regularly use the Internet. Interestingly, most of those also assert that the online media has created a positive impact on their lives and on society overall.

That would be great news two and a half decades following the release of the first ever Web browser called Mosaic by Sir Tim Berners-Lee. Today, there are various online browsers available to the public.

The poll was conducted in January and had 1,006 adult respondents. Up to 90% of those respondents personally think that the Internet has truly become a good and useful tool for them. Out of those respondents, up to 75% think that the online media have helped improve the society.

About 53% of the poll respondents think that it would be very hard for them to give up the World Wide Web now or in the future. Around 40% of the respondents assert that the Internet is an absolute necessity in their lives.

According to Pew Research, the Web has become instrumental in turning the online media from a mere data-transfer system into a mass-adopted technology. From specialists, it is now used not just by academics but also by hundreds of millions of ordinary people from all over the world.

According to the company s analysts, the Internet today is close to its saturation point, or 100% usage, especially in households that are generating at least $75,000 of income (99%), young adults aged 18 years to 29 years (97%), and college degree holders (97%). Interestingly, up to 68% of American adults now connect to the online media using their mobile devices like tablet PCs and smartphones.

It can be noted that Pew has been tracking online usage since 1995. Back then, just about 14% of Americans were using the World Wide Web.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.